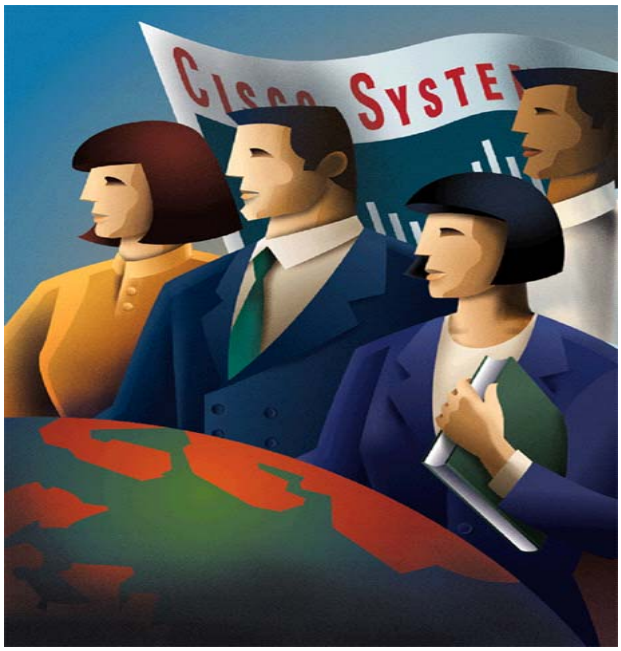


Cisco Systems' Response for

Global Aeronautic Network RFI,

Solicitation # NNC05ZVI011L

Request for Information

March 28, 2005

Table of contents

List of Figures

Executive Summary

"I truly believe that the Internet will change the way we work, live, play and learn in ways we are just beginning to explore. Our industry is maturing rapidly with the convergence of data, voice and video technology over one network. This convergence is creating a world in which technology is used to connect everyone to everything."

John Chambers, CEO, Cisco Systems

NASA is seeking to enhance the performance of the National Airspace System and to transform towards Network Centric Operations (NCO). The Networking Research Group of NASA's Advanced CNS Architectures and System Technologies (ACAST) project has formulated a list of requirements and design concepts to further ensure global interoperability and deployment. These requirements and design concepts are the building blocks for the proposed transformation.

The National Airspace System is a large undertaking intended to create a network interoperable over the global airspace, not just the National airspace. It must thus operate across networks owned and operated by various entities using whatever links become available, and accommodate mobile networks. Desired functionality includes the ability to perform Air Traffic Management over low-bandwidth links, integrate and share information traffic (situational awareness, passenger lists, aircraft maintenance, weather, entertainment, etc.) and have a common global security approach across air, ground, oceanic, and space systems. The ability to share network infrastructures, hardware, and protocols with other industries, and thus implement a cost effective Commercial Off-The-Shelf (COTS) solution is also desired. The system must also scale to support tens of thousands of aircraft.

The National Airspace System's success is dependent upon the integration and acceptance of several evolving technologies by different governments, industries, and consumers around the world. These technologies include IPv6, mobile networks, security, and multicasting. To evaluate the feasibility of this desired global system, NASA has requested industry input from outside the traditional aeronautics community.

Attached is Cisco's response to the RFI -- Global Aeronautic Network Requirements and Design Concepts. Topics discussed include mobile networks, IPv6 mobility, Home networking, NEtwork MObility (NEMO), multicasting, industry working groups, scalability, security, and briefly Network Centric Operations (NCO).

There are Organizational Conflicts of Interest (OCI) and Non-Disclosure Agreements (NDA) constraints that limit internal sharing of information and currently prevent the increased fidelity of our response. Additional information is available at: http://www.cisco.com/en/US/tech/tk872/tech_white_papers_list.html.

In summary, Cisco acknowledges the significant challenges facing NASA in designing and implementing a Global Aeronautic Network using off-the-shelf technologies in a manner consistent with network centric operations. Our response addresses many of these issues, requirements and design concepts, and offers the following conclusions:

- NEtwork MObility (NEMO) Basic Internet Engineering Task Force (IETF) Request for Comment 3963 standards track offers a building block for a Global Aeronautics network.

- There are currently many developments on-going in IPv6 networking in general and within the NEMO working Group at the IETF. The major focus areas are in Route Optimization for scalable NEMO networks and Route Projection and Home Agent (HA) functionality. These efforts are designed to make IPv6 mobile networks stable, offer fast convergence, and minimize messaging between routers.
- Coordination is needed between the IETF and the Institute of Electrical and Electronic Engineers (IEEE) standards bodies regarding Layer 2 (Wireless) and Layer 3 (Network) messaging needs
- Using the [1]DOORS protocol, we can today use IPv4 large scale Wide Area Networks (WAN) to carry NEMO IPv6 Mobile router traffic. This allows for spiral development of IPv6 mobile networks as well as testing new applications.
- Dynamic Virtual Private Networks (DVPN) are currently deployed in IPv4 networks today. This technology can be used as basis for IPv6 mobile security.

Considering the complexity of the issues and technologies involved, Cisco strongly recommends an iterative Government – industry dialog through the appropriate working groups and forums to ensure the best and most current technical information is available to make informed decisions. Cisco understands the information requested and released does not constitute a set of specifications or work statement for any contemplated agency contract. Further, the feedback provided in this document will not preclude Cisco from bidding on any future procurement with NASA, the DoD, FAA, or other U.S. Government entities. Cisco Systems, as the leader in IPv6 development, is ready to work with the global aerospace community on the development of a Global Aeronautics Network.

[1] Currently the DOORS protocol is implemented by CISCO and is proprietary; however, it is being considered by the IETF NEMO WG as a standard.

1 Network Centric Operations - An Overview

Network Centric Operations (NCO) is a real-time operation model based on mission-critical capabilities designed to securely deliver actionable information throughout the chain of command – anytime, anywhere – to achieve a competitive advantage.

Cisco is working with customers and partners to help them maximize this advantage. The results of the work will help transform the way they leverage information and technology to enable the next generation of Network-Centric Communications.

2 Requirements and Design Concepts – Feasibility

2.1 The Internet Today

Today's Internet resembles a traditional household carpet (Figure 1). To yield the reliability and day-to-day resilience consumers expect, it is engineered with a mesh that forms the solid framing upon which knots are assembled into coordinated, localized motifs. Similarly, the Internet Fringe consists of a dynamic network of nodes seeking connectivity to the core for shared service opportunities...

Figure 1. Carpet as Metaphor for the Internet. *Today's Internet can be thought of as a well engineered carpet mesh with a fringe of ad-hoc nodes relaying information across the mesh.*

In the case of the Internet, the Border Gateway Protocol (BGP) core forms the backbone, and the nodes are hierarchically organized into aggregations, forming autonomous systems wired together by physical links. Link States are distributed throughout the nodes that know all relevant states for their abstraction of the network. At the extreme, core routers recognize only highly aggregated prefixes, and do not have a default route.

This model of highly aggregated fully distributed core shows its limits, more by the size of the BGP core tables than in terms of the addressing capabilities of IPv4.

2.2 Intranets

The gating factor is not IPv4 addressing, but the development of so-called Intranets, and more generally, private networks. Even more than the introduction of Classless Interdomain Routing (CIDR), the concept of private networks has provided corporations with a wealth of addressing space that makes the Internet work today.

Intranets are organized around the shared Internet. The usage model is a client server from the Intranet to the Internet rather than peer-to-peer, which is limited by construction. Inside, an Intranet has the same structure as the Internet, and uses the traditional routing protocols for, and to, any connectivity. Yet Intranets are decoupled from the Internet, with Network Address Translation (NAT), [2]SOCKS, Transmission Control Protocol (TCP) relays, and proxy servers functioning as a gearbox. It can be argued that NAT has enabled the first model for the extension of the Internet.

2.3 Ad-Hoc Internet Connectivity, 'The Fringe'

A new form of connectivity is developing in the Fringe of the Internet. Nodes form loose, intermittent, ad-hoc meshes and relay traffic on-demand. In the Fringe, as opposed to the engineering and the trust model of the Internet (the carpet), the system is based on privacy and transparency. Nodes discover and share the Internet access dynamically, and share the services. This happens already at Home and within mesh networks. Mobile devices extend the Fringe dynamically, in an unpredictable fashion.

2.4 Routing (organizing) in the 'Fringe'

The Fringe is attached to the edge of the Internet, as shown in Figure 2. The base requirement is to find the nearest exit to the Internet infrastructure, and back. Nodes want to form trees that are rooted in the Internet and distribute the traffic within the Fringe. The trees must be self-forming, self-healing, and require little to no initial Authentication, Authorization, and Accounting (AAA) configuration.

Mesh Networking is forming stable local radio cores with some degree of inner engineering and security. Around the mesh, mobile devices are expected to form dynamic tree branches. Full privacy is imposed and no trust required. Within that space, a service such as connectivity might be obtained when it is guaranteed to be anonymous and transparent for both user and provider peers.

2.5 Internet 'Fringe' Conclusions

The growing Internet Fringe requires new models and new technical solutions based upon the anonymity and transparency. These solutions must adapt to a world of mobility and poor radio link quality.

The main objective of the Fringe involves forming trees to reach the Internet. Connectivity within the Fringe is also required to sustain local applications, dependant on the appropriate local services deployment to locate the people and the services.

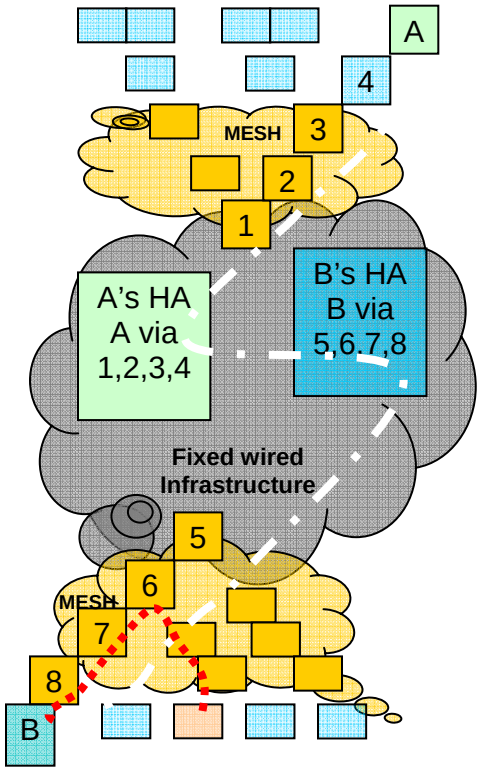


Figure 2. Routing in the Fringe.
Nodes form trees rooted in the Internet to distribute data in the fringe.

The NEtwork MObility (NEMO) working group at the Internet Engineering Task Force (IETF) has introduced the concept of Route Projection. Route Projection is a form of on-demand, peer-to-peer

[2] SOCKS is an "application-level proxy":

routing that forms tunnels to enable linking with routers in the Fringe and in the Internet. The end points of Route Projection might be fixed or mobile. The router peers exchange fine grained routes over their tunnel for a duration that is linked to its lifetime.

Route Projection with IPv6 enables the addition of a huge number of fine grained prefixes at no cost to the core BGP infrastructure. Single prefixes are only advertised to a few peers for a limited duration. Additional information is available at: http://www.cisco.com/en/US/tech/tk872/tech_white_papers_list.html

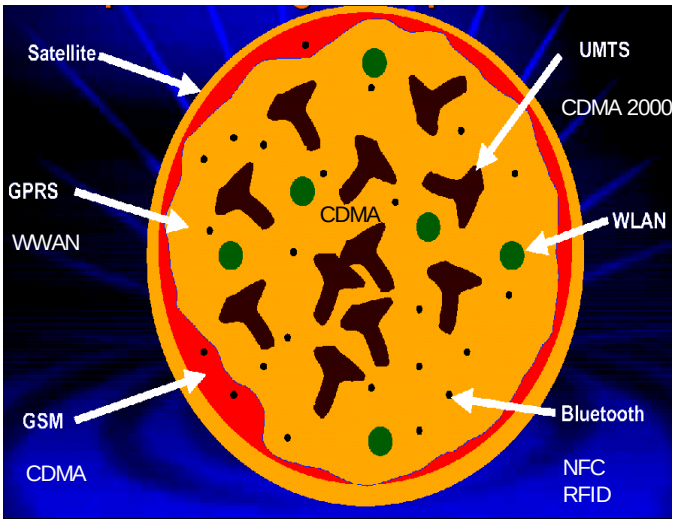


Figure 3. The Wireless World. *Several disparate wireless technologies co-exist providing a growing range of services.*

3 Mobile Networks

3.1 IP Mobility is Multi-Access

Many radio technologies are being developed or deployed today, as shown in Figure 3.

Handling mobility at layer 3 of the Open Systems Interconnection (OSI) seven layer model (Figure 4), enables the use of different available radio access technologies.

Different forms of wireless access provide different coverage and reachability service. IP mobility is across various types of access. This is why the selection of the access network must be available at upper layers.

Layer #	Identity
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Figure 4. The OSI Seven Layer Model. *Layer 3 provides optimal routing for messages to reach their intended destination.*

3.2 Transitional Roaming

IPv6 mobility is considered one potential enabler for IPv6. Mobile phones and other devices are huge consumers of addresses. Further, when IPv6 Network Mobility is enabled over an IPv4 Network, it becomes one more transition mechanism. Work has started at the IETF in that direction. In the meantime, Cisco has introduced the DOORS feature.

DOORS relates IP6 to IP4, and inherit its formats. A stateless gateway ensures the connectivity between the IPv6 and the IPv4 worlds, and the operation is transparent to the IPv6 core, including the mobility

related components. DOORS can traverse IPv4 NAT, Port Address Translation (PAT), and reverse NATs, but at the expense of a loss of security inherent to the Address translation in the IPv4 world.

3.3 Layer … and Sublayers?

It is a common practice since the days of Ypsilon and IP switching to break the layers and provide cross-layer services (Figure 5). The two most notable cross-layer services are "[3]SHIM" and cross breed.

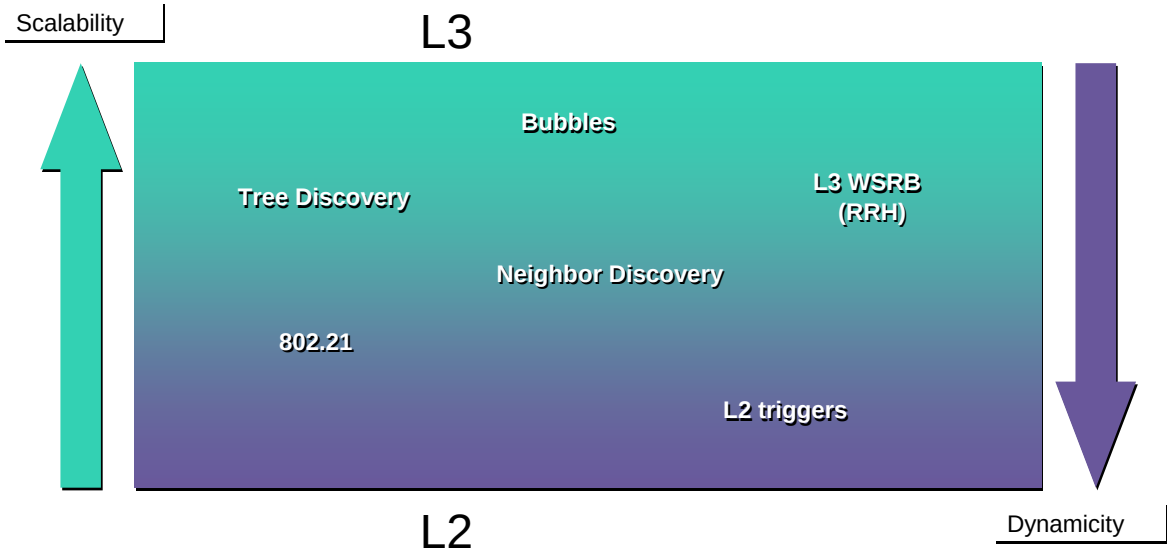


Figure 5. Cross-Layer Services. *A variety of cross-layer services are emerging that support mobile networks.*

The first type is an intermediate Shim layer that provides a common abstraction of the layer beneath for the layer above. The second type is a cross breed of layers where methods usually deployed at a given layer are reused at another layer to obtain similar benefits. Shim Layer and a cross breed examples are provided in sections 3.4 and 3.5.

Layer 2 (L2) reacts more quickly to the link events, and to processing packets with no link layer swapping. It is limited in scalability for a number of well-known reasons; including, broadcast issues, the lack of aggregation of the addressing, and the classical meltdown issue with Ethernet Transparent Bridging (ETB). It is not surprising in the context of quick mobility that some mix-and-match on L2 and L3 techniques are being proposed and implemented.

[3] "SHIM" refers to an intermediate thin layer.

3.4 Shim Layer

A Shim layer is an intermediate thin layer that occurs between two of the usual layers. The following are examples of shim layers:

⇨ **MPLS**: This is a virtual Layer 2 above layer 2 (e.g. L2.3) that establishes a mesh, which is useable by multiple protocols.

⇨ **802.21**: This IEEE WG is defining a "layer 2.5" that abstracts several radio types in order to provide a common interface to Layer 3 (IP) and make mobility decisions. This feature might prove very important if a number of radio type's pop up that can not be abstracted as Ethernet by IP.

⇨ **HIP**: The Host Identity Protocol, much like other MULTI6 candidates, is a Shim layer between L3 and L4. It provides an IP address to TCP that is used for naming rather than routing. HIP manages the real locators and hides them to TCP.

3.5 Cross Breeding

Cross breeding applies methods and techniques from other layers. There can be numerous types, and they are heavily used in the context of mesh. We can list the following examples:

⇨ **IP switching**: IP is being used to preset switching states. Several versions of this were deployed for the core when switching was faster than routing. In the Fringe, this could be Next Hop Routing Protocol (NHRP) based solutions setting up Dynamic Multipoint Virtual Private Network (DMVPN) interconnections.

⇨ **IP Bridging**: In the context of mobility, Loose Source and Record Route techniques, such as the Cisco Reverse Routing Header (RRH), can be seen as a Source Route Bridging on the Wireless network (WSRB), operated at Layer 3. The bridging operation is done at L3, based on IP addresses, when there is not a need for full fledge Interior Gateway Protocol (IGP) implementation.

⇨ **MAC routing**: Coping at Layer 2 with well known limitation of traditional transparent bridging (meltdown, broadcast), a process similar to a routing protocol can be introduced. This process proactively distributes the path to all Media Access Control (MAC) addresses in the mesh. Since MAC addresses are not routable, MAC routing is still limited in terms of scalability. (An example of that is Radiah Perlman's RBridges.)

⇨ **IP switching with Load Balancing**: IP routing is used to build one shortest switched path and a number of loopless paths where load balancing is performed at switching time. A measuring protocol is run independently of the routing in order to gather dynamic metrics and feed the forwarding stage. The Enhanced Interior Gateway Routing Protocol (EIGRP) and Resource Reservation Protocol Traffic Engineering (RSVP-TE) permit this to some extent.

3.6 Movement Detection

Traditional routing and bridging are not designed for mobility. Transparent Bridging states are very slow to establish and avoid the meltdown syndrome, and most routing protocols will collapse if the link flaps and the nodes change their points of attachment. Further, as the interface with the radio is inherited from Ethernet, there is no provision for mobility related Application Program Interface (API), and an L2 roaming operation will often occur unknown to the network layer.

To adapt to mobility, a node must first detect when it occurs, control it if possible, and act on the movement to restore the connectivity. With IPv6, a number of means have been introduced to the network layer to detect the movement. Making this detection as fast as possible is the core of the activity

at the IETF Detecting Network Attachment (DNA) WG. In particular, L3 has indirect delayed tools to compensate for what L2 did not signal when the event occurred.

3.7 L3 Timers

IPv6 routers advertise themselves using Router Advertisement (RA) messages. These messages are L3 beacons, emitted at a regular interval. When monitoring the beacons, a mobile node might simulate that it stayed at a given location and can still use a local address built from a prefix advertised by that router.

MIPv6 has allowed a faster rate for sending RA, and has added an RA interval option to the RA message. It takes up to 2.5 times the RA interval to detect the advertising router is no longer reachable and conclude that a movement has occurred.

3.8 L3 Link ID

The DNA problem covers the movement between links. When any hint comes in, the node attempts to decide whether it is still attached to the same link or not. Routers on the same link might not advertise consistent network information, so adding a new link identifier at layer 3 could help make that decision.

3.9 L2 Triggers

The 802.21 WG has started the L2 triggers' work for link availability. L2 triggers are indications from L2 about a link event that just occurred or might occur soon. A short list of L2 triggers defined by 802.21:

- ⇨ Link up/down
- ⇨ Link going up/down
- ⇨ Link Quality threshold
- ⇨ Trigger rollback
- ⇨ Link secured (EAP, VPN)
- ⇨ Better signal quality AP available

In general, the most useful L2 trigger, Link Up/Down, can be related to the association state in 802.11 with the PDP context in GPRS, and with the IPv6CP state in 2GPP2.

3.10 Attachment Router Selection

When movement is detected, or if new information is obtained about the routers available in the vicinity, a Mobile Node might decide to select a new attachment router. The Mobile Node will select the new Attachment Router as its default gateway, and auto-configure a new address from a prefix advertised by that router. There is a need for a quick, loop-free selection of the attachment router.

3.11 Reachability

If the roaming decision is left to the layer 2 while visiting some unknown radio domains, it will pick up the best radio signal, regardless of the network attachment. It is critical to consider what can be reached via an attachment router, as opposed to what's the best signal. A roaming decision made by a shim layer 2.5 might be even worse.

One Application Processor (AP) might give access to the fixed Internet connection, while another is carried by a private home that is disconnected from the Internet at that point in time. Mobile Nodes need clues to form a shallow tree rooted at the Internet AP.

3.12 L3 Triggers

An L3 trigger conveys the reachability information that a given access provides for Layer 3 users. This information is a key factor for a roaming device to make its selection. L3 triggers should provide a way to distinguish a disconnected home network or a local Mobile Ad Hoc Network (MANET) with a bunch of nodes connected, from an Internet access (i.e. a public access point or a city mesh).
Ideally, an L3 trigger is a form of beacon and an L3 to L3 message that does not need a response.
The beacon advantage is the possibility of not requiring a radio association to be usable. It could take a number of routing protocol exchanges to get the full picture of the reachability that a given access provides.
A short list of L3 triggers:

- IPv4 IRDP, IPv6 ND (No Discovery)
- IPv6 ND extensions:
  Visit www.ietf.org and insert the following links:

  For plain host and for multi-homing,
- draft-ietf-ipv6-router-selection-03.txt provides reachability information in a routed topology.

  For Mobile Nodes
- draft-ietf-dna-link-information-00.txt allows movement detection when switching AP

  For Mobile Routers (MRs)
- draft-thubert-tree-discovery-01.txt builds the shallowest tree of MRs to the Infrastructure (and much more)
- Routing Protocols

  IGP, MANET

3.13 AP Selection Heuristics

Reachability is the key to making L3 roaming decisions. Serviceability will be the gating factor for upper layer control.

A mobile node makes its attachment decision based on the capabilities of the candidate Access Router in terms of reachability expressed in L3 triggers.

In the case of 802.11, the selection of the AR decides which ESS the mobile node wishes to join and the client radio has to select the best AP for that ESS in terms of a radio signal. Roaming within an ESS can be done transparently to the L3 control. The client can use secondary metrics that orient the choice for joining and/or forwarding, as provided by 802.11k.

The interface up/down trigger is the most useful. The other L2 triggers might be difficult to map into L3 protocol actions. In terms of security, EAP might indicate whether the client is attached to a trusted zone and simplify the VPN behavior of the stack.

3.14 IPv6 Host (client) Operation

An IPv6 host maintains its Default Router List (DRL) as part of the IP stack. To perform the selection optimally, the IP layer needs to get all Router Advertisements from all potential Access Routers via all radios. *Note: this is not assured today with 802.11, as RA messages are considered as data and transmitted as class 3 messages, which can only be received after association.*

Based on triggers (interface up/down, RA messages), recent history, and metrics (L3 hops, aggregated bandwidth, L2 metrics), the host might revisit the DRL and order it from the most preferred to the least preferred for roaming, and be ready to make a choice quickly.

An IPv6 host also auto configures one or several addresses from the prefixes found in RAs. One of these addresses will be used as a CareOf address for IP mobility.
Now the host needs to multicast packets over the Attachment Router's link and send packets to that router. It still needs to receive L2/3 triggers from other routers available on the same physical interface, regardless of the association states.

3.15 IPv6 Attachment Router (AR) Operation

An IPv6 Access Router exposes a local prefix for visitors in Router Advertisements and proposes its services as default Gateway. It could be used by a Mobile Host as its temporary Attachment Router.

In terms of 802.11 radio, the AR might be remote from Access Point and there could be more than one AR on the ESS, and more than one L3 protocol. The AP needs hints in order to select specific messages as triggers and send them before association as class 1 or class 2 messages.

3.16 Mobile Router Case

A Mobile Router acts as a Host on the roaming interface (called egress interface in the NEMO specifications), and as a Router on the Mobile Network interface (ingress), exposing the Mobile Network Prefix in the RA messages. A Mobile Router can act as a Mobile Access Router (MAR) for other MRs to attach with in a nested NEMO configuration.

A Mobile Router can provide various forms of interconnections, depending on the required service.

- ⇨ Internet via WWAN or WLAN
- ⇨ MANET via WLAN
- ⇨ Intranet vs. Internet detection for VPN

The automation of that process dependency on the application still needs to be defined for various Mobile Network Nodes.

3.17 Technical Conclusions

Currently the support for Nested NEMO operations is limited by the 802.11 layer, which is opaque to the L3 triggers for nodes that are not associated, and hides most of the roaming opportunities to Client Nodes already associated.

The model for a Mobile Router to provide access services for one another has to be defined, proven and accepted across service providers.

We are looking for coordination between IETF and IEEE to enable L3 control for reachability aware roaming.

4 IPv6 Mobility

From IP phones to game consoles, billions of new devices are becoming IP aware, with or without the need and ability to provide their own mobility. This increased range of IP awareness has resulted in a need for increased addressing space and improved Plug and Play networking capabilities. These trends encourage the deployment of IPv6 and intermediate boxes to provide mobility for devices with limited networking capabilities.

4.1 IP Mobility

4.1.1 A Driver for IPv6

Currently there are more than 1.5 billion mobile phone users globally. There are not enough IPv4 addresses to make them reachable at all times. We also observe the creation of a Pervasive Networking and computing fabric – the Fringe -, is composed of handheld devices, medical diagnostic systems, automotive gateways, etc.

Available Technology and local rulings have enabled radio data communications to become widely available to the public. This availability allows users to access the Internet via mesh networks as they move around in cities across the globe. They can couple their cell phones to their PDAs, and then use Public 802.11 Wireless Access, via mesh networks, for connectivity.

The ability to remain constantly connected at the same network identifier enables the emergence of a new breed of applications that include push services (stock alerts, sports updates) and peer-to-peer networking (multimedia messaging and voice integration).

IP Mobility and IPv6 are designed to respond to these requirements. Coupling them appears to be an even better idea because Neighbor Discovery has built in mechanisms for a faster Movement Detection and for Address Auto Configuration. IPv6 is faster in movement than IPv4 and doesn't require a Foreign Agent, which enables Service Providers to deploy more widely.

Most of the progress in the mobility space in the standard bodies is happening in the context of IPv6. 4G telephony is considering IPv6 for mobile IP telephony, and vehicular consortiums in the world (Car2Car in Europe, InternetCar in Japan) have adopted IPv6 for car-to-car communication.

4.1.2 IP Mobility Summary/Opinions

The Internet today is not fully ready for IP mobility. Even if IPv6 can exist over an IPv4 fabric as a transitional method, a good portion of network attachment detection (DNA WG at IETF, L2/3triggers, 802.21, 802.11r, 802.11k) is still under development.

Mobile IP is transparent to the routing fabric, but it is highly related to the multiple types of wireless access and can not ramp-up until wireless high speed networks are widely deployed. Business models and applications are still to be defined. IP mobility also has to face the competition of alternate solutions, such as, Host Identity Protocol (HIP) and Session Initiation Protocol (SIP).

In terms of deployment, it must be considered that IP mobility enables new flows that impact the wireless infrastructure: Telephony over IP (latency, Quality of Service (QoS) and P2P (always on, multimedia).

5 Network Mobility

5.1 Basics of Network Mobility

5.1.1 Host Mobility vs. Network Mobility

Mobile IPv6 really deals with Mobile Hosts as opposed to any form of IP Nodes; including, Routers. Moving Routers around entails moving the attached networks and it takes some additional signaling to get there. NEtwork MObility (NEMO) defines the operations of a Mobile Router (MR) handling the mobility of a whole network on behalf, and transparent to, all the nodes attached to that network.

5.2 What is NEMO?

The NEMO Working Group is concerned with managing the mobility of an entire network, which changes as a unit, its point of attachment to the Internet and thus its reachability in the topology. The Mobile Network includes one or more MRs, which connect it to the global Internet.

”A Mobile Network is assumed to be a leaf network; i.e., it will not carry transit traffic. It could, however, be Multi-Homed, either with a single MR that has multiple attachments to the Internet or, by using multiple MRs that attach the mobile network to the Internet.”

The NEMO IETF Working Group Charter is available at the following link:
http://www.ietf.org/html.charters/nemo-charter.html

5.2.1 Practical Use Cases

A number of cases were envisioned for a network that moves as a whole. The degree of global and relative mobility varies from one case to another.

Case 1) A Home Gateway provides global connectivity for the appliances in the house with minimum IPv6 support. When it is NEMO enabled, it provides a stable range of addresses for the network at home, and enables a seamless operation in terms of networking if the family relocates. Service Providers have to decide whether an economical model can be based on an ‘always reachable network’ as opposed to ‘application specialized services’ based on SIP.

Inside the home, visiting friends and family might connect to the Network and share the facilities for local gaming and Internet connectivity. The Visitors might want to be reachable using their own Home Address and manage their own mobility. The Home Gateway, which is a Mobile Router, accepts visitors that are also mobile. We will see if this situation results in a nesting of tunnels, which has a number of negative consequences for the traffic in terms of path and latency, and it requires a specific NEMO Route Optimization.

A radio mesh can be used to relay the traffic between the various rooms. Layer 2 mobility might be enough to handle the movement from room to room, but specific features, such as Cisco’s [4]SWAN architecture, will be required to enable a good roaming time for voice.

Case 2) A Personal Area Network (PAN) connects various wearable devices and body systems (e.g. bio-monitors) together, as in Figure 6. A portable Mobile Router (MR) provides a global reachability for all these devices, but low battery consumption is required for access and usable autonomy.

[4] SWAN is Cisco’s Structured Wireless-Aware Network.

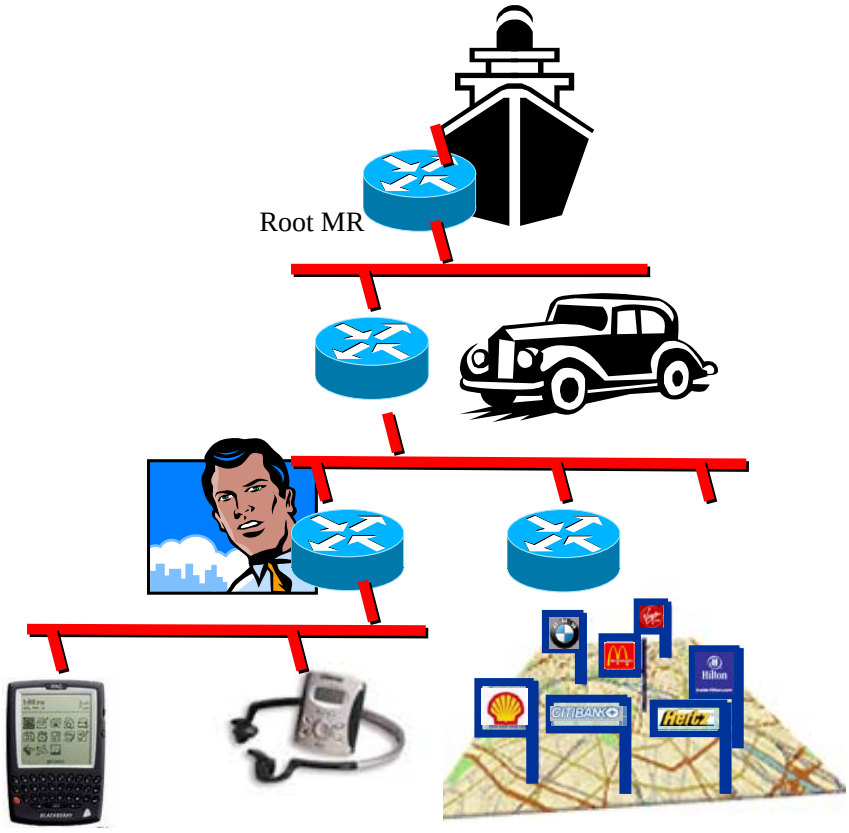


Figure 6. Personal Area Networks and Mobile Routers. *Networks of Mobile Routers with nested hierarchies enable an expanded range of services.*

The MR needs low-power connectivity close to its environment. It will connect to the Home Gateway when at home, and then to buses, airports, cars, planes, trains, hotspots…etc.

This creates a nested hierarchy of MRs, for instance: PDA → PAN → Vehicle → Ferry.
The order that nodes attach to each other is strictly based on the role of each entity and follows the hierarchy. In our specific example, it makes no sense for the ferry to attach to a PAN, so the system must be properly engineered and provide the mechanisms to enforce the rules.

The nesting happens between entities of different types; as a result, the degree of nesting is limited to the order of 2 or 3. Each level of hierarchy might be operated by a different service provider, so the use case wants a meta-provider that integrates the services of multiple ISPs and presents a single access and billing to the final users.

A user in a train might connect to the train's Mobile Network, obtain a local address from that Network, and visit the Internet to find local services during a stop at a station. The client might hear a better signal from the station, but it would cause the loss of its active connections. If the client manages its mobility, this would result in a simple roaming, and preserve the continuity of the operations. On the other hand, if the client has a way to maintain the connection with the train network regardless of the best signal, he will get a continuous service throughout the travel. This reminds us that there are other heuristics than plain signal strength for making a roaming decision.

Case 3) The European Car-2-Car consortium and, the InternetCar in Japan are working on the definition of inter-vehicular communication. This might mean car-to-car communication and packet relaying. In the latter case, cars organize themselves as a community, helping each other to enable a global service that will benefit all of them.

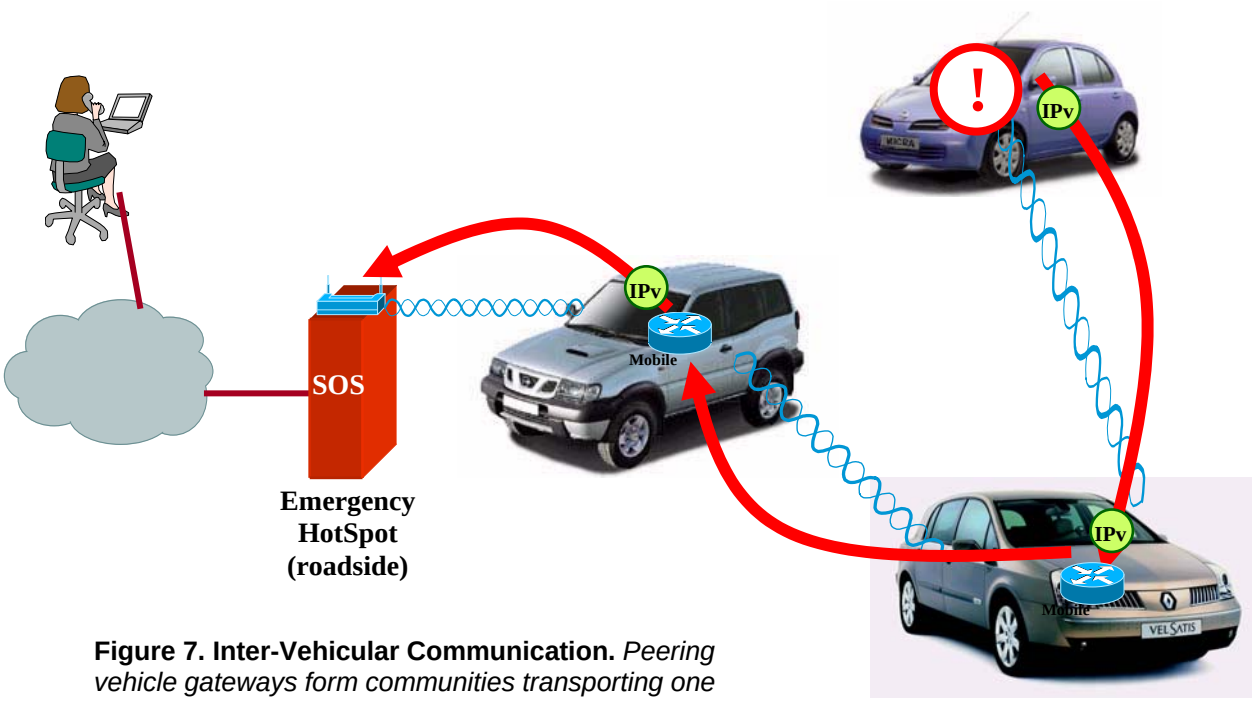


Figure 7. Inter-Vehicular Communication. *Peering vehicle gateways form communities transporting one another's packets over networks of variable depth.*

There is a wide consensus that this inter-vehicular communication should be based on IPv6. In this case, vehicle gateways transport each others packet, acting as a community service. Unlike the previous example (**Case 1**), all devices are of a same kind and the network can reach an arbitrary depth.

A typical use case is a traffic jam with thousands of immobilized cars. Most are too far from a public access point to be able to communicate, but jumping over a few cars they might be able to get there. Also, a geographically localized broadcast might be very useful to signal the jam to vehicles arriving at full speed.

5.2.2 Object Model and Terminology

Mobile Router (MR):
A router capable of changing its point of attachment to the network while moving from one link to another link. The MR is capable of forwarding packets between two or more interfaces, and possibly running a dynamic routing protocol modifying the state by which it forwards packets.

A MR acting as a gateway between an entire mobile network and the rest of the Internet has one or more egress interface(s) and one or more ingress interface(s). Packets forwarded upstream to the rest of the Internet are transmitted through one of the MRs egress interfaces. Packets forwarded downstream to the mobile network are transmitted through one of the MRs ingress interfaces."

MObile NEtwork (NEMO):
NEMO is an entire network that is moving as a unit, which dynamically changes its point of attachment to the Internet and its reachability in the topology. The mobile network is composed of one or more IP-subnets and is connected to the global Internet via one or more MRs. The internal configuration of the mobile network is assumed to be relatively stable with respect to the MR.

Note that the definition of a NEMO describes it to be a complex structure with routers that are fixed with regards to the moving topology, and more than one Mobile Router assuming the mobility for all. In that case, the network moves as a solid, and, in particular, the MR should not split.

Mobile Network Node (MNN):
An MNN is any node (host or router) located within a mobile network, either permanently or temporarily. MNNs can be either a Local Fixed Node (LFN) or a mobile node (VMN or LMN)."
Note: The LFN is the proverbial 'plain' IPv6 node, with no support of MIPv6 or NEMO. In particular, it can be a Router, which mobility is handled by the MR. A visiting MN handles its own mobility, and unlike a Local MN, it is not Homed in this NEMO.

Correspondent Node (CN):
This is a term for any node that is communicating with one or more MNNs. A CN could be located within a fixed network or within a mobile network, and could be either fixed or mobile."

Currently, the definition of a Correspondent node comes from Request for Comment (RFC) 3775 and was not modified with RFC3963, since Route Optimization is not covered. In the future, NEMO might need to impact the CN functionality for its own Route Optimization, or introduce the concept of a Correspondent Router that terminates NEMO.

5.2.3 Basic Operations

NEMO has produced its initial RFC (RFC 3963) to specify the extensions to MIPv6 for Networks in Motion. Also called the NEMO Basic Support, this RFC describes the Mobile Router operation to register to a Home Agent, establish a tunnel, and request that the Home Agent install the routes to the Mobile Network Prefix(es) (MNP) over that tunnel.

Two modes of operation have been initially specified, with a third mode under development.

- ⇨ It is expected that both ends have a prior knowledge of the MNPs associated to each given MR in implicit mode. That mode requires a double configuration (on MR and HA) and could leave configuration errors undetected till runtime.
- ⇨ The Mobile Router provides its list of MNPs as a new option to the Binding Update messages in explicit mode. The HA must have a way to check a MR for authorization of a MNP before it accepts a binding.
- ⇨ Additional work in underway to enable the third possible mode of operation, where the HA centralizes the configuration and delegates the prefixes to the MRs at bootstrapping time or for checking in runtime.

After the tunnel is installed and the routes are set up, the operation in the HA is similar to that prescribed by MIPv6 with a routing twist, which places NEMO in a half position between a layer 2 and a layer 3 operation. When the HA gets a packet from a CN to a MNN, it performs a traditional route lookup and decides the packet is routed via the MR Home Address (HA), and creates a local delivery. The packet exits the fast path and is passed to layer 2. Alternately, the Neighbor Cache look-up finds a MIPv6 Binding Cache Entry (BCE), and the packet is finally tunneled to the CareOf Address of the Mobile Router.

Ideally, the initial route lookup would have pointed to the MRHA tunnel and the processing would have been done in fast path. However, the layer 2 nature inherited from Mobile IPv6 forces the Neighbor Discovery operation at layer 2, in case MR would be at Home. This might be even less probable in the case of NEMO than it is with MIP and accounts for one of the reasons why it is so highly desirable to evolve NEMO into a fully layered 3 process.

A Home Network is mostly flat. In front of the Home Agent you might find millions of MRs, each one with a fine grained prefix. This creates potentially millions of routes to configure and a very large routing table with no possible hierarchy. In order to alleviate that burden, Cisco has introduced the concept of generic routes. A generic route is expressed as a single CLI entry, but it represents virtually all the routes to all the Mobile Network Prefixes (MNPs) in a Network.

Generic Routing expects a regular expression between the Mobile Network Prefix behind a Mobile Router and the suffix of the Home Address of that Mobile Router. In practice it means something like; for all ”x,” “HOME”:x::/64 is routed via “HOME”:”LINK”::x. The route lookup has been extended to extract an “x” of the number of bits from the prefix of the destination, and apply a mask to the suffix of the Home Address to compute the MR address.

5.2.4 Recursive Use (nesting)

RFC 3963 did not attempt to address the concept of Route optimization. In fact, the concept is far more complex with NEMO than it is with MIP. The results are seen in NEMO basic support being far from optimized, and a nested configuration with MRs attaching to MRs, which complicates the situation more. Reference Figure 8.

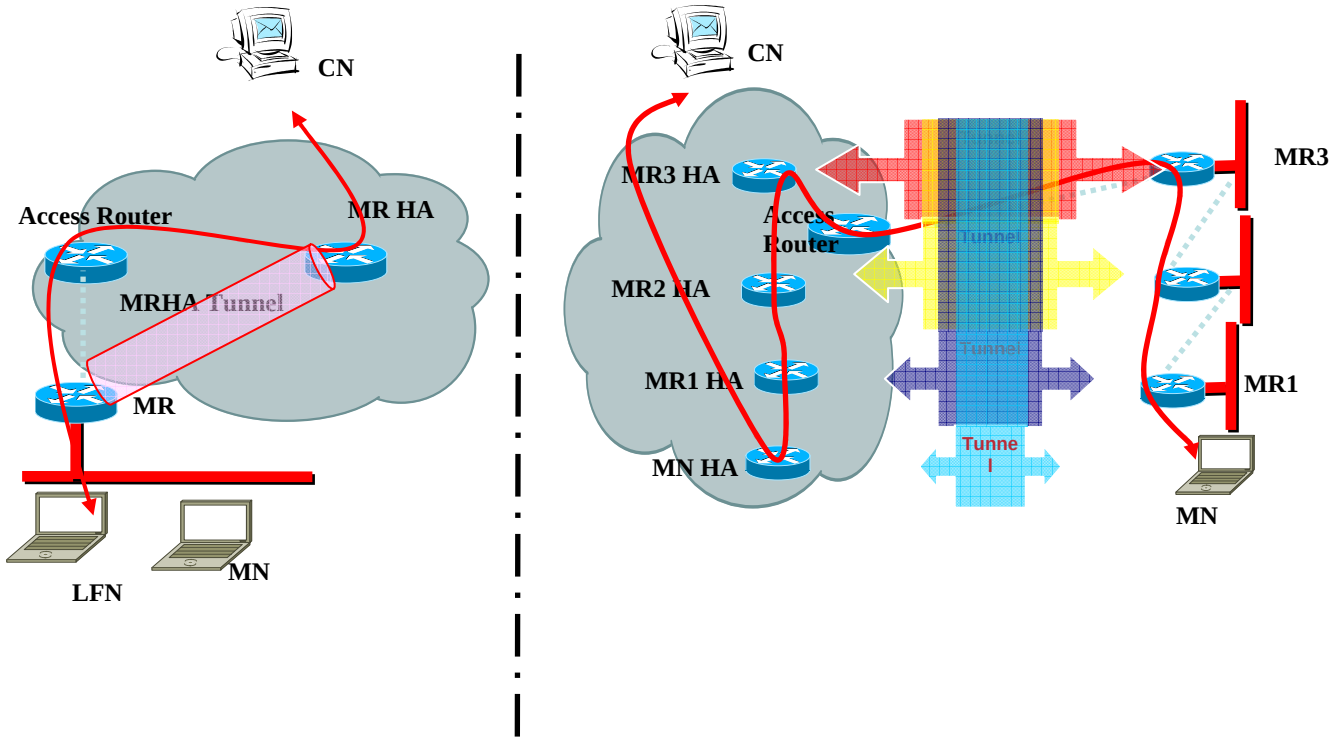


Figure 8: Recursive Nesting. *Nested configurations result in longer Internet paths and transport delays.*

When NEMO Basic Support packets are tunneled back and forth between the MR and the HA, a longer route in the Internet is created, and results in an increased delay. In a nested configuration, packets will bump into all the HAs of all the MRs in the path. This effect is often referred as pinball routing.

Since NEMO is based on a RFC 2472 tunnel (IPv6 in IPv6), each packet is pre-appended with a full IPv6 header. This overhead increases the processing delay in the HA, and increases the chances of fragmentation. Each level of nesting causes an additional IPv6 header.

If a Visiting Mobile Node (A MIPv6 MN not at Home in the Mobile Network) manages its own mobility, it will be subjected to the sub-optimality of the NEMO Basic Support and its Route Optimized packets will be tunneled to the Home Agent of the Mobile Router.

5.2.5 What about NEMO?

Can we consider NEMO simply the adaptation to IPv6 of Cisco's MR for IPv4? It is more complex.

- ⇨ With IPv6 Neighbor Discovery and its MIP adaptations, roaming is quicker than with IPv4/DHCP. The difference is 20 seconds versus 2 seconds in speed. Additional mechanisms are under study and development to gain more speed and reach acceptable figures for voice applications.

- ⇨ In terms of topology, NEMO has no concept of Foreign Agent, but we might see regional boxes dedicated to Local Mobility Management, MIP proxying, and other technologies to alleviate the current limitations of the protocol

- ⇨ IPv4 is pervasive, but IPv6 access is low in numbers at the moment. The Mobile Router for IPv6 needs a transition mechanism for IPv4 traversal. Cisco's DOORS is this type of transition mechanism.

- ⇨ With the larger number of addresses brought by IPv6, a new model of aggregation based on Service Providers delegating prefixes to their customers was put in place. The same numbers enable a given customer to buy services from several ISPs; however, he gets as many prefixes as ISPs, and using the wrong one might not pass ingress filtering at the SP edge. This situation is called MultiHoming in IPv6 and was studied at the Multi6 WG at the IETF. With NEMO the situation is even worse, and a number of additional situations might occur (e.g. An MR with multiple CareOf Addresses, multiple Home Agents, or a Mobile Network with multiple MRs).

5.3 Nemo Technical Conclusion

NEMO enables Mobile Networks to be reachable and topologically correct. More importantly than this, NEMO is the first technology to be standardized around the concept of Route projection. As a result, in explicit mode, the MR establishes a tunnel dynamically with its Home Agent and advertises its fine grained routes over that tunnel. We anticipate the concept of Route Projection to be fully achieved, depending on how RO is specified.

NEMO basic support still has a number of limitations. It is still half L2 and half L3 and does not allow a globally distributed Home (HAHA protocol). It is still missing a model for Local Mobility Management. A DHCP PD based solution was proposed but it has no Delegation model and has no transition model from IPv4, however Drafts are under discussion.

NEMO basic support is suboptimal. It lacks a model for Global Route Optimization (global HAHA, Correspondent Routers, NEMO Proxies, etc.) and for Nested Route Optimization. A number of solutions have been proposed; e.g. Tree Discovery with Reverse Routing Header, or a MANET with a specific Gateway.

NEMO has introduced a number of interesting problems and numerous Internet Drafts were published to study these problems and propose initial solutions. At the moment, there is intense activity in the standard bodies to decide the final direction needed to answer all the scenarios.

6 Home Network in NEMO

6.1 The concept of Home Network

The MIPv6 Home is a subnet on a physical link. It is tied to a physical link by the Neighbor Discovery related operations. With NEMO however, the Home Network becomes an aggregation. Home *is not necessarily* contained on a Home Link (e.g., Extended Home Network) and can be deployed in a number of variations.

With NEMO, the Home Link can also be virtualized. This configuration can be deployed when MRs do not need to return Home, which was not a problem for most use cases we considered. The single HA constraint can be fixed by an inter Home Agents Layer 3 protocol, such as HAHA.

6.2 Home Network Models

In the various dispositions proposed hereafter, an aggregation is partitioned into Mobile Network Prefixes and disposed in various fashions. The aggregation is generally called Home. Home is advertised into the infrastructure by the Home Agent(s), and might or might not be installed on a Home Link.

The NEMO Basic Support is, by design, very open to future extensions and has deployment possibilities. The organization of the Home Network is one example.

6.3 Extended Home Network

The MIP Home Network is conserved as one subnet of a larger aggregation that encompasses the Mobile Networks. This aggregation is called an extended Home Network as seen in Figure 9.

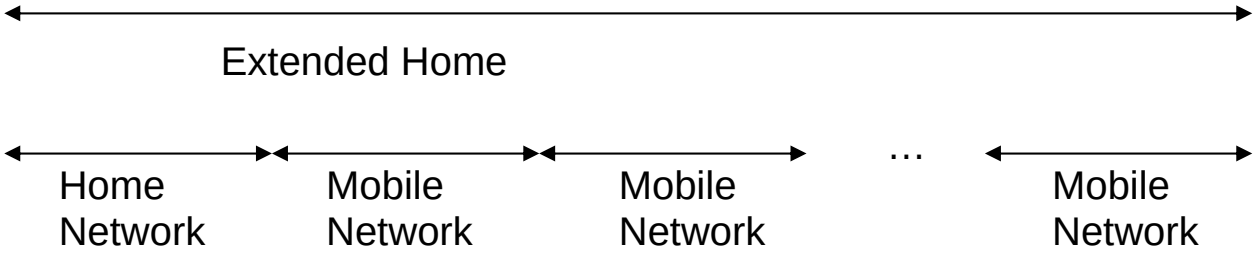


Figure 9. Extended Home Agent: *Distributed HAs allow for scalability of mobile networks.*

A Mobile Router performs its normal routing operations between the Home Link and the Mobile Networks to maintain the MNP routes in the absence of a binding when at Home, as shown in Figure 10. The HA is configured with static - or generic - routes to Mobile Network Prefixes, or, alternatively the MRs recognize home and connects to the local IGP.

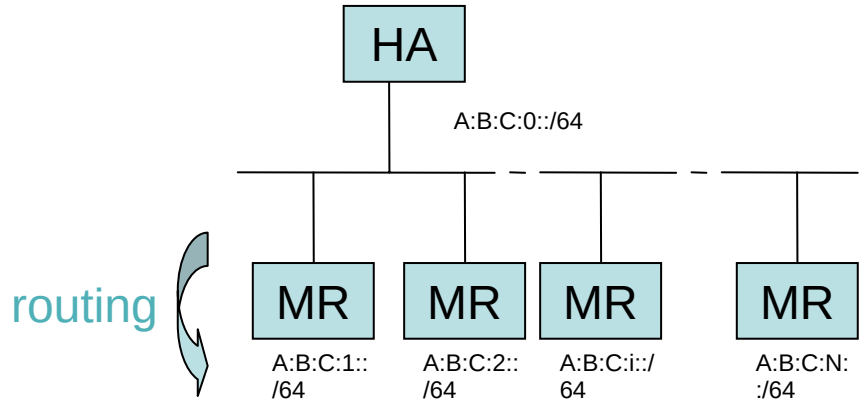


Figure 10. *Mobile router at Home*. *Mobile routers use Interior Gateway routing when at Home.*

Only the Home Network inherited from MIP is installed as the subnet on the Home Link, which all Mobile Nodes (hosts and routers) take their Home Address. NEMO allows a Mobile Router to use an address from its own MNP as a Home Address in the Extended Home Network disposition. This does not seem to be the most natural operation because it requires an additional support by the HA to declare the valid range of Home Addresses.

The generic routes model implies that the MRs get a Home Address from the subnet on the Home Link. Extended Home Network with generic routes is the recommended model for large deployments since it minimizes the configuration, the size of the routing table, and the impact of bindings to the local routing fabric.

6.4 Aggregated Home Network

In this scenario as shown in Figure 11, the Home Network actually overlaps with the Mobile Networks. The full aggregation is configured as the prefix on the Home Link to enable any address from any MNP to be considered by the HA as a valid Home Address with no additional configuration.

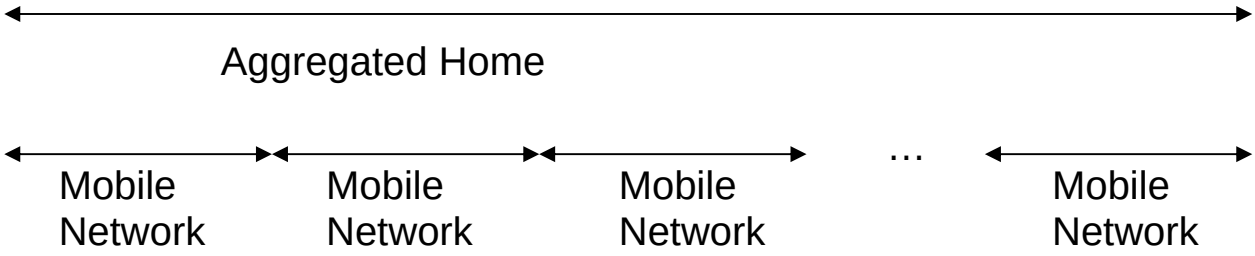


Figure 11. Aggregated Home Network. *Mobile routers are attached to a network of Home agents to form an aggregated home network.*

In this disposition, the Home Agent expects all the Mobile Network Nodes to be on link; therefore, no need is expressed for a static route or an automated participation to the local IGP when a Mobile Router is at Home. In return, when the MR is connected to the Home Link with an Ingress Interface, it needs to

switch automatically to a bridging mode between the Home Link and the Mobile Networks. In terms of routing, this disposition is an aberration.

When this automated bridging operation is not available on a given implementation, it is possible to connect the MR to the Home Link with the Egress Interface(s) to make all MNNs directly available to the HA without any bridging. See Figure 12.

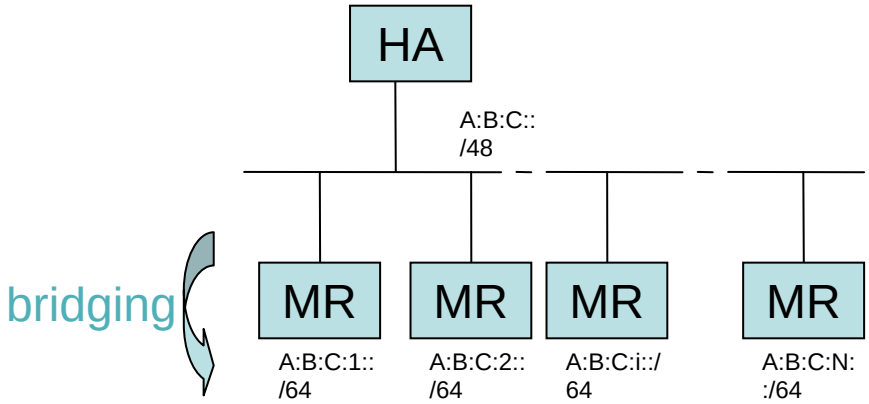


Figure 12. Automatic Bridging for Mobile Routers. *Mobile routers are at Home with Bridging*

In this scenario, it is very possible for a Mobile Router to use its address on its MNP as a Home Address for binding purposes. In that case, the Duplicate Address Detection (DAD) operation that MIP mandates on the Binding Cache creation is moot since the real prefix is not on link.

If configured for Aggregated Home Network, an implementation would optionally verify the Home Address matches (one of) the MNP(s) associated with that MR, and skip the DAD process.

6.5 Mobile Home Network

A Head HA advertises the global Home to the infrastructure and attracts all the packets from the outside to tunnel them to the MR that is responsible for the next level of hierarchy. The next MR de-encapsulates and re-encapsulates the packets to the next MR down the logical tree. This process is repeated till the destination is reached.

An example of a Command Line Interface (CLI) for a Cab Company is in Figure 13. The Cab Company has offices distributed in the largest cities in the US and has equipped the cabs with MRs homed to the closest office from their location of operation. We take the example of the San Francisco (5F0) office.

```
interface Ethernet0
 ip address 10.0.2.1 255.255.255.0
ipv6 enable
 ipv6 nd suppress-ra
 ipv6 mobile router-service door

interface Ethernet1
ipv6 address CAB:C0:CA5A:CA5A::CA5A/64
 ipv6 enable
 ipv6 nd ra-interval msec 1000
 ipv6 mobile home-agent run

ipv6 route CAB:C0::/32 CAB:C0:CA5A:CA5A::FFFF generic extension 16
ipv6 route CAB:C0:CA5A::/48 CAB:C0:CA5A:CA5A::FFFF generic extension 16
```

Headquarter of Cab Company: CA5A

```
ipv6 mobile router
 home-network CAB:C0:CA5A:CA5A::/64 discover
 home-address home-network ::5F0
 home-door 10.0.2.1
 register lifetime 90

interface Ethernet0
 ip address dhcp
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd suppress-ra
 ipv6 mobile router-service roam try-the-door

interface Ethernet1
ipv6 address CAB:C0:5F0:5F0::5F0/64
 ipv6 enable
 ipv6 nd ra-interval msec 1000
 ipv6 mobile home-agent run

ipv6 route CAB:C0:5F0::/48 CAB:C0:5F0:5F0::FFFF generic extension 16
```

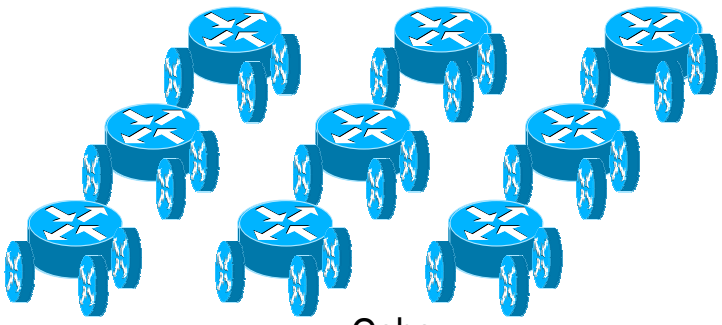
San-Francisco Office: 5F0

```
ipv6 mobile router
 home-door 10.0.2.1
 home-network CAB:C0:5F0:5F0::/64 discover
 home-address home-network ::CAB1
 register lifetime 40

interface Ethernet0
 ip address dhcp
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd suppress-ra
 ipv6 mobile router-service roam try-the-door

interface Ethernet1
 ip address 10.0.1.1 255.255.255.0
 ipv6 address CAB:C0:5F0:CAB1::CAB1/64
 ipv6 enable
 ipv6 nd ra-interval msec 1000
```

SFO's Cab N°1



Cabs

Figure 13. Example CLI for Cab Company. *Configuration commands for NEMO.*

In this configuration, each level of the Mobile Home Network CAB:C0::/32 is also an Extended Home Network. The Head Home Agent, CA5A, acts as a DOORS gateway to accept bindings over IPv4. The generic route to CAB:C0::/32 allows traffic distribution to all the offices. The CFO office and the cabs are configured to use DHAAD, and IPv4 traversal is enabled. MRs, e0 is the egress interface, and e1 is the ingress interface and the Home Link on HAs. This is how IPv6 works.

6.6 Distributed Home Network

The distributed Home Network model splits Home in different geographies, breaking the Home Link paradigm, shown in Figure 14.. This can not be achieved with the NEMO Basic Support which is still tied to the Layer 2 by its MIP inheritance. In order to achieve the Distributed Home Network model, NEMO must become a full layer 3 technology.

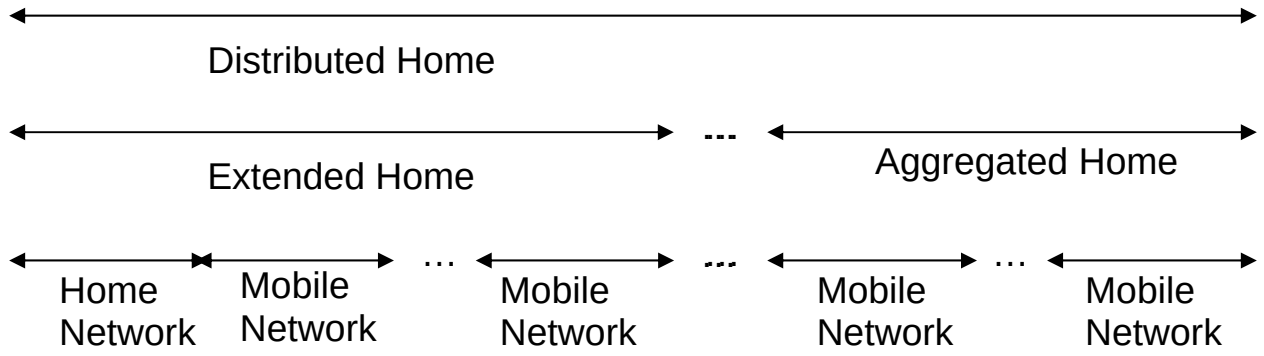


Figure 14. Distributed Home agents. *Distributed HAs require full layer 3 routing for NEMO.*

The global distribution of Home Agents is useful when a Mobile Router moves a geographically large area; such as, airplane, vehicle, etc... If a Mobile Router moves far away from its Home Agent, the overhead of the basic NEMO, caused by the bi-directional tunnel, can not be ignored. With the distribution of Home, the Mobile Router establishes its tunnel with the closest Home location, and the routing information is distributed over the mesh of tunnels between the HAs, as a form of Route Optimization. Referenced in Figure 15.

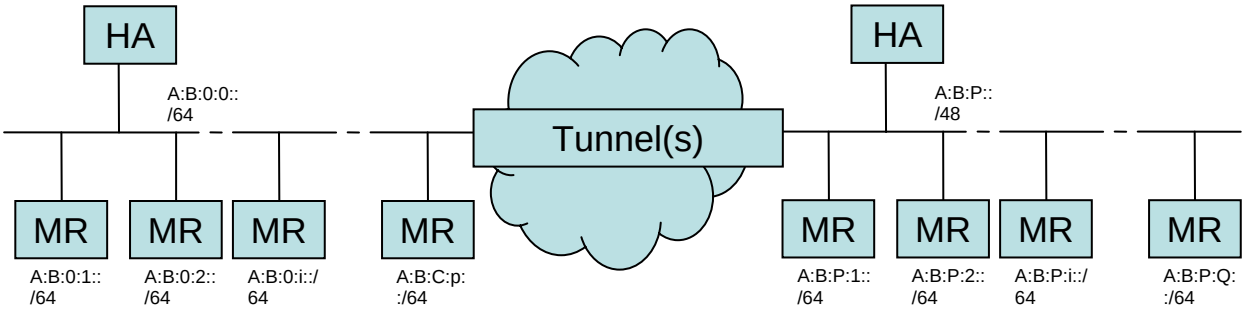


Figure 15. Global Distribution of Home Agents. *Global distribution of HAs provide for scalability and load balancing.*

This distribution is also effective for scaling and load-balancing. A global Home might have multiple sites and each one is composed of a number of Home Agents. Bindings are distributed over the HAs, and redistributed by a routing protocol.

The Distributed Home Network requires layer 3 coordination between the HAs to setup a mesh of tunnels and establish routes over them, which is another form of Route Projection. This is the core of the global HAHA protocol that has been presented to the IETF.

6.7 Virtual Home Network

A Virtual Home Network is a specific case where the Home Link is not a physical link. In fact, this model is applicable to both MIP and NEMO. In the NEMO case, all of the previous models apply. The Home Link can be configured on a loop-back interface, or on an automatic (point to multipoint) tunnel, which resolves the other tunnel end point dynamically using the Binding Cache.

The Virtual Home Model provides a higher availability of the Home Link, but an external system like HSRP should be put in place to ensure high availability of HA itself, which was partially covered by the HA discovery and DHAAD mechanisms. There is no returning Home for the Mobile Nodes on a virtual link.

Another advantage of the Virtual Home Model is that it saves all the ND related link layer activities (HA discovery, DAD, proxy ND). As a result, the HA could operate fully at layer 3, preserving the fast path and the associated performance while the latency due to the DAD mechanism in the initial binding disappears. This results in more efficiency throughout the whole HA process.

There is no HA load balancing, as provided by standard MIP, unless a new HA to HA layer 3 protocol is introduced. There is also no returning Home for the MRs and the tunnel must be maintained at all times with the associated incurred overheads in frame size and latency.

6.8 Home Network Summary

NEMO brings a new dimension to the MIP concept of Home Network, making it an aggregation opposed to a final subnet and enables multiple deployment possibilities. The full capabilities of all deployment possibilities are not necessarily available with all implementations; and, a Service Provider will want to compare the supplier's solutions and recommended configurations, for specific capabilities. This is especially important for scalability, high availability, and load balancing.

Home is one of the areas where there is still a lot of work in progress and expected benefits, especially for scalability and Route Optimization with the introduction of the HAHA protocol.
There is a lot more to do with NEMO than current achievements, and we are still working on terms of services and deployment.

The choice of the model for Home is expected to be critical for a specified deployment. It might be beneficial to consider if a Home Link must be physical or virtualized, and how the growth of the service will translate in terms of number of Home Agents, control traffic, and routing stability in the local IGP, e.g., inter HA traffic on the Home Link, Neighbor Cache entries, etc.

7 Work In Progress at NEMO

7.1 MultiHoming

The HA might want to check an MNP for a unique Mobile Router registration. If the Home Address is constructed out of the Mobile Prefix, it ensures that a Home Address is unique. It might be desirable for redundancy reasons, however, that two MRs share an ingress link, and both register the same prefix at the same time with different Home Addresses, which are guaranteed unique by the DAD mechanism on the shared ingress link.

- How can the HA make sure that they are actually connected, and keep moving as a solid and never split?
- What would happen if they did?
- How does the HA balance the traffic to the MNP over the two available tunnels?

An additional test was proposed at the NEMO Working Group at the IETF to verify that activity. Two MRs registering for the same prefix, pinging via one of the MRs the Home Address of the other one, and becoming connected by their Ingress Interface that carries the prefix. Home itself could be MultiHomed, causing the MR to support more than one prefix. This problem is quite similar to the traditional site MultiHoming. A Mobile Router might wish to maintain more than one tunnel, with more than one Home Agent, and from multiple CareOf Addresses at the same time.

We have seen a lot more cases with NEMO MultiHoming than with Site MultiHoming, which is not an easy problem. This is why the MULTI6 Working group at the IETF rejected consideration of the MultiHoming problems related with mobility.

7.2 Route Optimization

7.2.1 The Problem

In Figure 16, we see a nested configuration with a Visiting Mobile Node (VMN) attached to a Mobile Router (MR2), and MR2 is attached to Mobile Router MR1. This could represent a friend in your car that is located in a parking lot. The signal is relayed by another car to the hotspot in the supermarket, and your friend might be shopping, or even ordering things to be delivered to your car.

By way of the NEMO Basic Support, MR1 establishes a tunnel with its Home Agent and installs its default route over that tunnel, and so does MR2. The result is MR1 encapsulating all packets from MR2 and sending them to it's HA. Finally, by means of MIPv6, our VMN establishes a tunnel with its Home Agent and installs its default route over that tunnel.

To reach a supermarket that is two 802.11 hops away, all the packets from VMN are encapsulated the first time by VMN itself and then by MR2, MR1, and all packets out of MR1. This totals four IPv6 headers in a row. In the case of a voice sample for IP telephony, the size of a packet, as it takes its last 802.11 hop to the hotspot, it can be multiplied between five and ten times!

Fortunately you live in town and your Home Agent is on your Home Network, at your home. However, the car you happen to be using to relay your packets is from the other end of the country, and your visiting friend lives on the other side of the ocean. As a result of the outer encapsulation, all packets crossing the country are de-encapsulated by HA1, then travel back a few blocks away to your Home and are de-encapsulated by HA2 – your HA -, then crossing the ocean again they are de-encapsulated by HA-VMN, to eventually come back to the supermarket in line with your car. This is what we call pinball routing (Figure 16) when a packet is bouncing across the Internet from Home Agent to Home Agent.

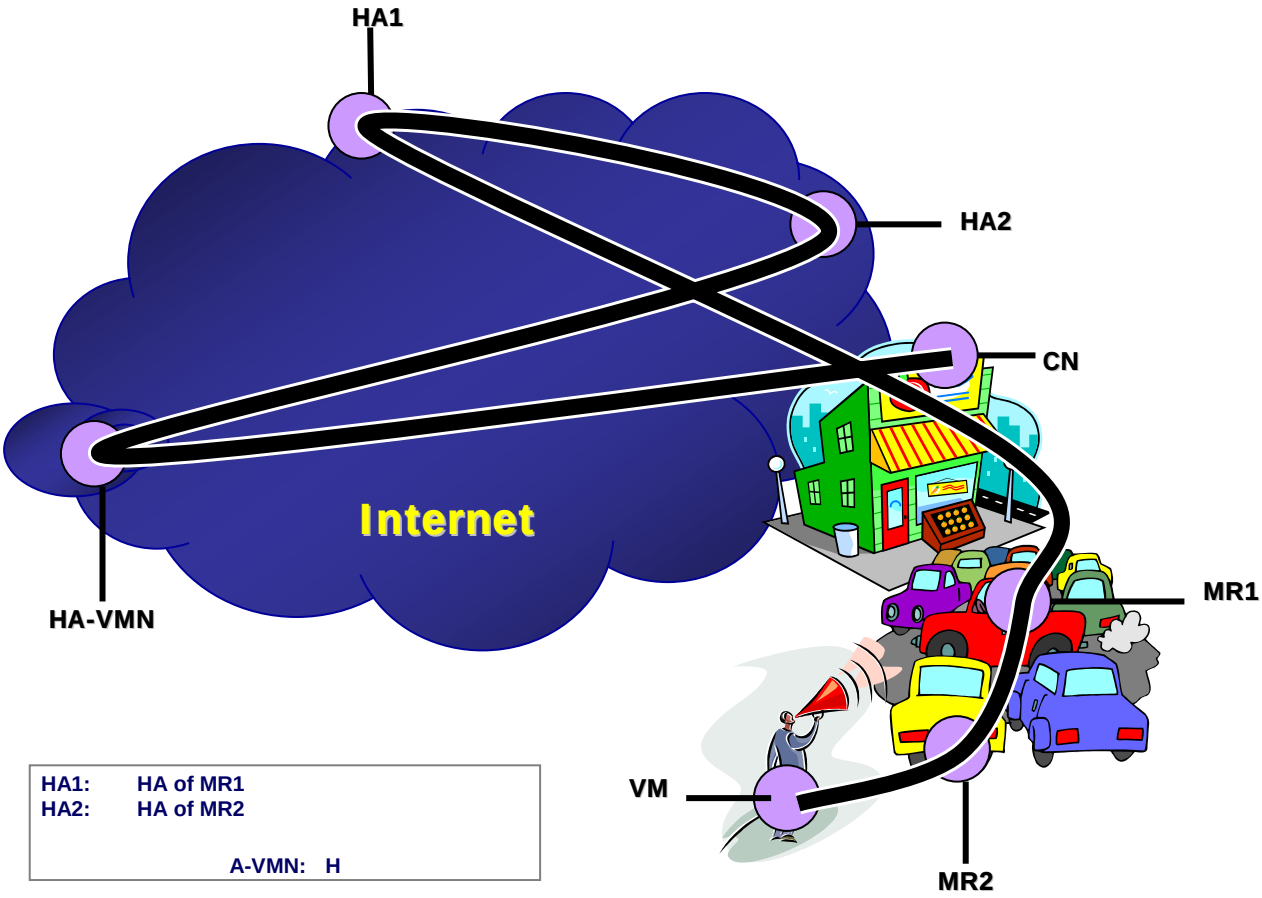


Figure 16. Pinball Routing from HA to HA: *MR1 must send traffic to HA1 to communicate with MR2. This is not optimal.*

In each of the three Home Agents in the route of the packets, they must leave the fast path in order for the router to perform the Binding Cache lookup. When we add this to global travel, the latency incurred by this incredible travel makes it incompatible with voice communications.

For a larger packet, the three levels of encapsulation might cause a fragmentation. If one fragment is lost and the rest of the packet makes it all the way, it is then lost in the reception buffers.

If the supermarket offers hotspot services for its site only and does not relay packets to the Internet, your friend and yourself cannot connect Home and all shopping is totally impossible.

7.2.2 The Issues

We understand why Route Optimization is critical for NEMO. It is even more critical than for MIPv6 because of the amplification effect of nesting. Many drafts were published to propose solutions to various aspects of the NEMO RO at the same time the Basic Support was developed and we learned about a number of potential caveats.

⇨ **Location privacy**: In some use cases, e.g. 4G IP telephony, privacy is a critical factor. Your CareOf address would give your location away and it should not be disclosed to the other party.

- **Trust**: With NEMO Route Projection, the other end needs to trust a Mobile Router for the ownership of its Home Address, and for a Mobile Network Prefix, which is much more complex to prove end-to-end, but do-able in the infrastructure.

- **Nested Complexity**: In a nested NEMO configuration, when a sub-tree moves away, all the Binding Caches for the correspondent side tunnel end points need to be updated with all the hops in the new attachment tree. The new attachment router, where the sub-tree moves in, has a difficult time discovering and binding with the end points of existing tunnels started in the sub-tree. For the previous attachment point, it is also difficult to figure out which states it should stop maintaining. The correspondent end-point might have difficulty in correlating all the states in a given nested path.

- **Binding Update Storm**: When a sub-tree moves in, as all tunnel end points are updated at the same time, a brutal flow of control messages is issued at the same time, and it is critical to avoid the loss of the packets. If each hop must send a BU for each tunnel, then the problem is even more critical.

A summary was made as a taxonomy and problem statement draft.

The location privacy and trust issues need a solution within the infrastructure as opposed to end-to-end. In that space, solutions based on Correspondent Routers, and solutions based on proxies (HAHA protocol), were proposed.

The nested complexity and the BU storm issues demand a single binding per tunnel, even in a nested configuration. MANET and source Routing Based Solutions (RRH) have been proposed at this point. It will be up to the Market, in particular to Service Providers, to make the final decisions, based on the recommendations by the IETF and the features proposed by the Suppliers.

7.2.3 Split and Conquer

In our example, the final goal of RO would enable your friend to connect to the supermarket and do his shopping whether the supermarket is connected to the Internet or not. This might require a local routing structure of some form. Some intermediate goals could be; bypass the Home Agents, avoid any double tunneling, etc.

The Route Optimization problem space can be split into four possible types:

- **RO for nested mobile network:** When an MR2 is attached behind an MR1, a second level of tunneling does not bring any value in terms of security, but, has a cost in latency, packet size, etc… in fact, it is unsafe for MR1 to bring packets from MR2 inside its own Home Network, and this should be avoided in the general case. Some forms of (MANET) routing inside the nested NEMO allows reaching MR2 from the supermarket. In the icher versions, they would also enable your friend to order from the supermarket without connection from the infrastructure.

- **RO with visiting mobile host:** An MIPv6 Mobile Node might not share new protocols, and MIP packets will still be re-encapsulated even if we prevent MRs from re-encapsulating other MRs packets. This second sub-problem is to avoid re-tunneling for MIPv6 endpoints as well.

- **RO with Correspondent Node:** If the previous problems are fixed, we end up with a single tunnel, between the nested end point and its Home Agent. The equivalent of the traditional MIPv6 RO for NEMO happens if the Correspondent Node is enabled to terminate NEMO tunnels as well.

- **RO within routing infrastructure:** Since NEMO deals with routes over tunnels, it might make more sense to deploy a Correspondent Side Router (CR) that terminates the tunnel for the flows destined to the CN and performs the necessary routing on behalf of the nodes. The NEMO RO could happen completely within the infrastructure if proxy Home Agents were disseminated around the globe for

mobile clients to connect to, handling the primary bindings to the HA on behalf of the MRs, and handling the secondary bindings to CRs or other proxies for route Optimization. The global HAHA protocol that we discuss is a solution for that specific problem.

8 Multicasting

8.1 HAHA

At the core, the HA to HA protocol replaces the Neighbor Discovery based MIP interaction between HAs. The objective is to eliminate the Home Link. The result of suppressing the Home Link would be Home becoming virtual, with the consequences that have already been discussed. We have several reasons for doing this.

8.1.1 Multihoming

If Home is not tied to a Link anymore, it becomes possible to distribute it geographically, e.g., airports, large cities, etc. Geographic distribution would enable worldwide roaming users to re-Home close to their current location.

8.1.2 Scalability

We have seen that ND based operations, and the associated concept of a Home Link, limits the scalability of Home. With HAHA, Home Agents are distributed, either locally in a site or globally across the Internet, and sets up a routing fabric over a mesh of tunnels.

8.1.3 VPN

It is a classical feature for VPNs to allow the roaming users to connect to the closest point-of-presence into their company VPN. The same feature can not be provided with MIPv6 or NEMO because the Home has a unique physical location.

8.1.4 Route Optimization in the Infrastructure

If an MR can locate and bind with a HA, or a proxy HA close to its current location, the distance (MR-proxy -HA) is contained and the associated overhead is globally limited. When a CN sends a packet to the MR, if it finds a (proxy) HA or a correspondent router that terminates the tunnel nearby, the overhead (CN, CR) is contained as well, as illustrated in Figure 17.

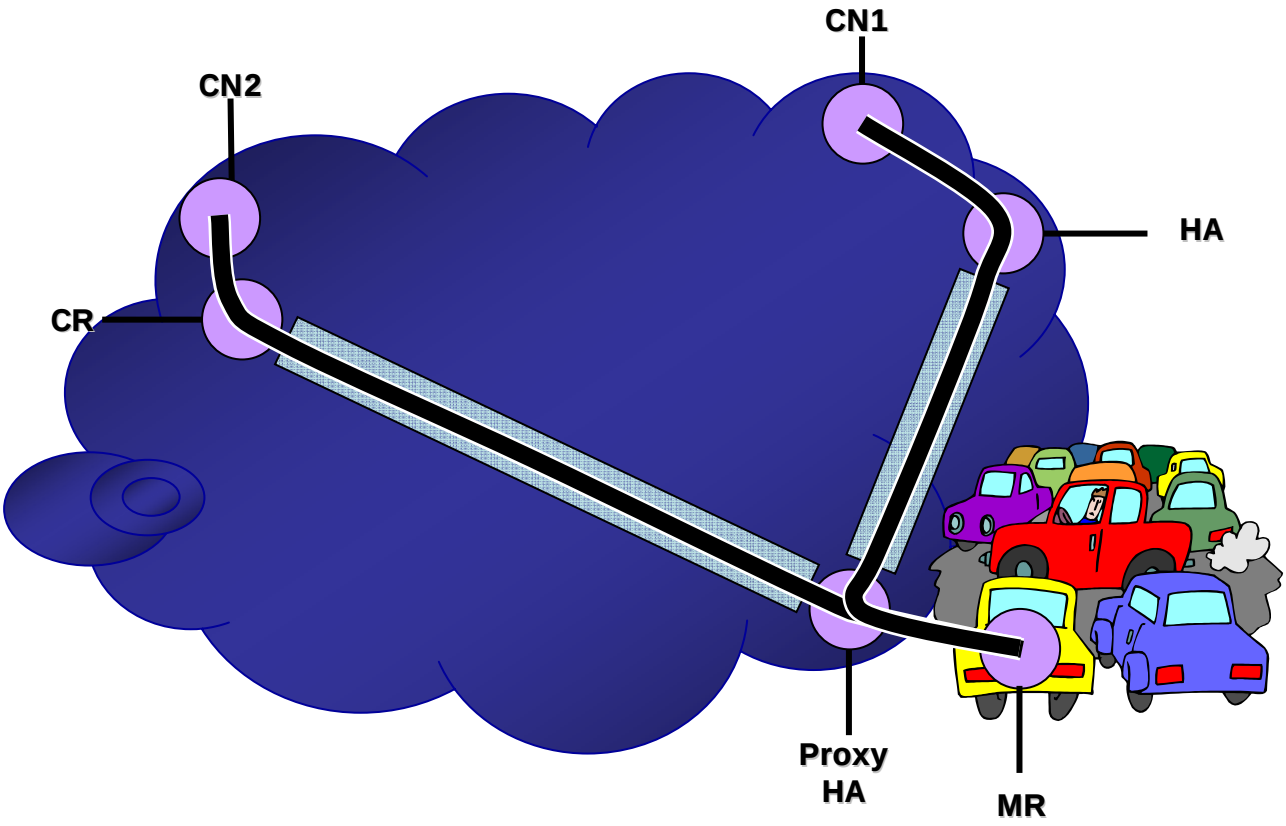


Figure 17: Proxy HA Part of Route Optimization: *The Mobile Router uses the closet Proxy HA for bindings*.

With HAHA, an MR binds to a proxy that handles a primary binding for a HA from MRs Home and secondary bindings with other entities (HA, proxy, CR) closer to the correspondent. If those entities are widely distributed, we can reach a high degree of optimization for the Infrastructure part of the NEMO RO problem.

9 Applicability of Industry Standard Technologies and Protocols

9.1 Standard Bodies

A number of standard bodies work with IRTF, IETF, and IEEE on data mobility related issues. Some of those issues are discussed below:

9.1.1 MIP4 IETF WG

IP mobility started at IETF with the works by Charlie Perkins on IPv4 and produced a number of RFCs, starting with RFC 2002 to 2004. We have seen few actual deployments. Cisco proposes a standard compliant Home Agent, as well as a proprietary, pioneering implementation of Mobile Router for IPv4, which was one of the bases for the NEMO work in IPv6.

9.1.2 MIP6 IETF WG

Mobile IPv6 has taken quite a long time to come up in its final form, RFC 3775 and RFC 3776. The upfront inclusion of a secure Route Optimization technology in the absence of a generalized Public Key Infrastructure was time consuming. Additional work is underway to improve the degree of trust for specific cases where a PKI could be available.

9.1.3 MobOpts IRTF WG

Additional Optimizations are being studied and standardized at the Mobility Optimizations WG. In particular, work related to faster L3 roaming (Fast MIP) and to Local Mobility Management (HMIP), is on the way to experimental RFC.

9.1.4 NEMO IETF WG

NEMO is a WG at IETF that deals with Network Mobility and the concept of a Mobile Router for IPv6. NEMO has produced a number of drafts, some turning into informational and standard track RFCs. The NEMO Basic Support (RFC 3963) extends Mobile IPv6 for MRs, without Route Optimization.

9.1.5 802.21 IEEE WG

The 802.21 WG at IEEE works on a radio layer abstraction for multiple radios. It will provide a shim layer between L2 and L3 (a L2.5) that could handle mobility on behalf of L3. Part of this work is defining L2 and L3 triggers to help upper layers cope with mobility.

9.1.6 802.11k IEEE WG

802.11k relates to the same types of issues. It defines L2 information that could be useful for L3 in the specific case of 802.11.

9.1.7 DNA IETF WG

The Detecting Network Attachment (DNA) is a newly formed group at IETF. DNA focuses on L3 tooling design is to improve the MIPv6 movement detection and make it faster. This is tightly linked to IEEE work

9.1.8 MANET IETF and IRTF WGs

The MANET problem is too wide to translate in a single RFC. Currently, 4 RFCs have been produced by the IETF and new protocols are being studied at the IRTF counterpart. A specific adaptation for the needs of the Fringe is considered by the MANEMO list.

10 Scalability

For IPv6 mobile network to scale to thousands of nodes it must have low session overhead, fast convergence, allow for multiple communications paths, and be secure. The proposed NEMO IETF standards are moving in this direction. The use of Route Optimization and RRH allows for the low overhead and fast convergence.

It must be noted that most implementations today are for very few nodes and that full scale deployment of IPv6 NEMO is still in development. There have been some network simulations that show NEMO with RO and RRH are very scalable.

11 Unified Security – Air Mobile, Ground, Oceanic, and Space

11.1 IPv6 Peer to Peer Security using Certificate based Object Identity

Within IPv6 Peer-to-Peer mobile networks, the major issue is the Security Policy Database (SPD). The SPD in a peering network, using traditional methods of IP addresses, does not scale well. For example, a 500 node IPv6 peering mobile network would have, without any optimization, 499 security policies per router. This allows every router to securely communicate with every other peer router. This does not include the SPDs for hosts or applications.

Cisco is currently looking at taking some of our developments for Dynamic VPN in IPv4 and applying this feature to IPv6 peering networks.

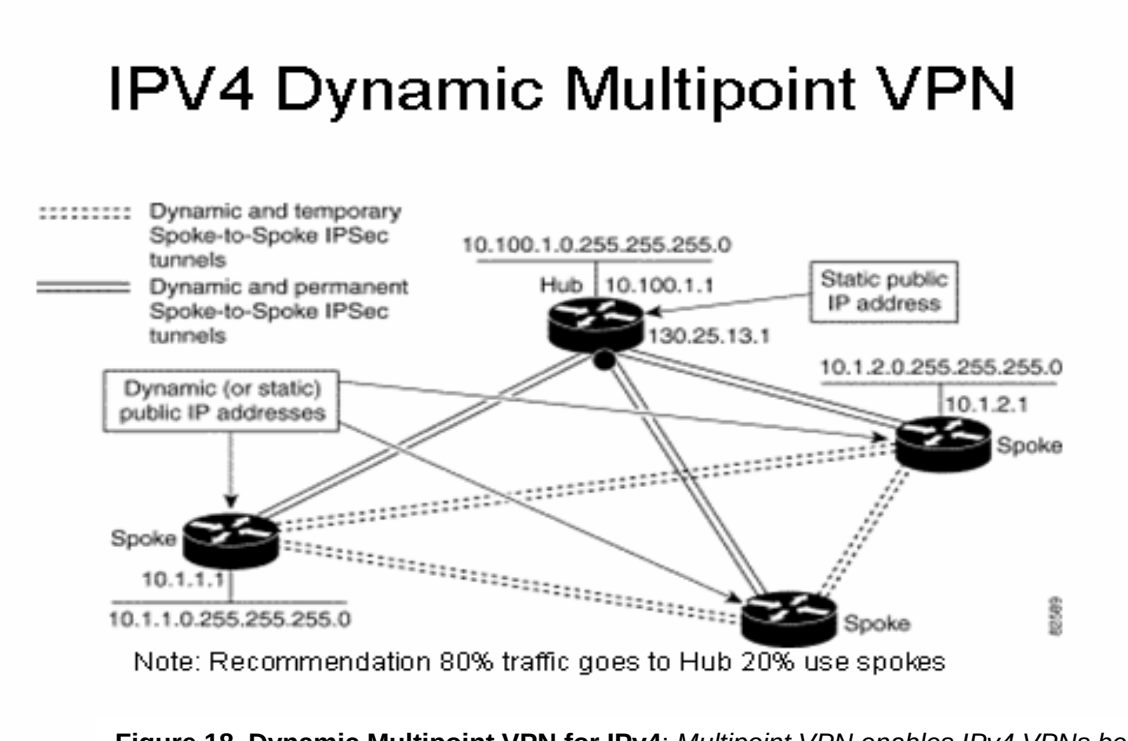


Figure 18. Dynamic Multipoint VPN for IPv4: *Multipoint VPN enables IPv4 VPNs between routing peers.*

Using a Certificate based system will enable the use of the objects identity for the SPD. There will be no need for static defined IPv6 addresses. This also enables the use of Public Private Keys with Certificates to establish trust and identity. Encryption will use these keys. The keys reduce the security policy database and are independent of the IPv6 addresses. Once authenticated, the router keeps track of its nearest neighbors. When neighbors have been authenticated to the HUB Certificate Authority, the router can be a peer since it also has been authenticated to Certificate Authority (CA). Trust is established through CA chains. The router needs to know only its nearest neighbors using this chain. This reduces processing and network overhead and can be used at layer 2, layer 3, and possibly higher layers.

A Certificate can be added or removed from the IPv6 Peering network without changing or adjusting the router's general identity. Obviously there is overlap, and the use of (Online Certificate Status Protocol

(OCSP), RFC 2560) servers, PKI-AAA, etc., or other revocation/authorization mechanisms. This technology leverages existing certificate standards in IPv4 networks and allows for a very scalable IP peering network. Multiple Certifications can be used for multiple levels of security from link layers, network layers, applications layers to user level**.**

DVPN knowledge from IPv4 can be used for IPv6 implementations**.** Certificate based security mechanisms are scalable and flexible enough for IP peer-to-peer mobility.

12 Acronyms

2GPP2 - Second Generation Partnership Project 2

AAA - Authentication, Authorization, and Accounting

API - Application Program Interface

AR – Access Registrar

BCE - Binding Cache Entry

BGP - Border Gateway Protocol

CA - Certificate Authority

CIDR - Classless Interdomain Routing

CLI – Command Line Interface

CR - Correspondent Side Router

DAD - Duplicate Address Detection

DMVPN - Dynamic Multipoint Virtual Private Network

DRL – Default Router List

DNA - Detecting Network Attachment

DVPN – Dynamic Virtual Private Networks

EAP - Extensible Authentication Protocol

EIGRP - Enhanced Interior Gateway Routing Protocol

ESS - Electronic Switching System

ETB - Ethernet Transparent Bridging

GPRS - General Packet Radio Service

HA - Home Address

HA-VMN - Home Address-Visiting Mobile Node

HIP - The Host Identity Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IGP - Interior Gateway Protocol

IRDP - ICMP Router Discovery Protocol

LFN - Local Fixed Node

MAC – Media Access Control

MANET - Mobile Ad Hoc Network

MAR - Mobile Access Router

MIP - Mobile Internet Protocol

MNN Mobile Network Node

MNP Mobile Network Protocol

MR Mobile Router

MRHA - Mobile Router/ Home Agent

NAT - Network Address Translation

NCO - Network Centric Operations

NEMO - NEtwork MObility

NHRP Next Hop Routing Protocol

OCSP - Online Certificate Status Protocol

OSI - Open Systems Interconnection

PAN - Personal Area Network

PAT - Port Address Translation

PDA - Personal Data Assistant

PDP - Packet Data Protocol

QoS - Quality of Service

RA - Router Advertisement

RSVP-TE - Resource Reservation Protocol Traffic Engineering

SIP - Session Initiation Protocol

SPD – Security Policy Database

SWAN - Cisco Structured Wireless-Aware Network

TCP - Transmission Control Protocol

VMN - Visiting Mobile Node

VPN - Virtual Private network

WG - Working Group